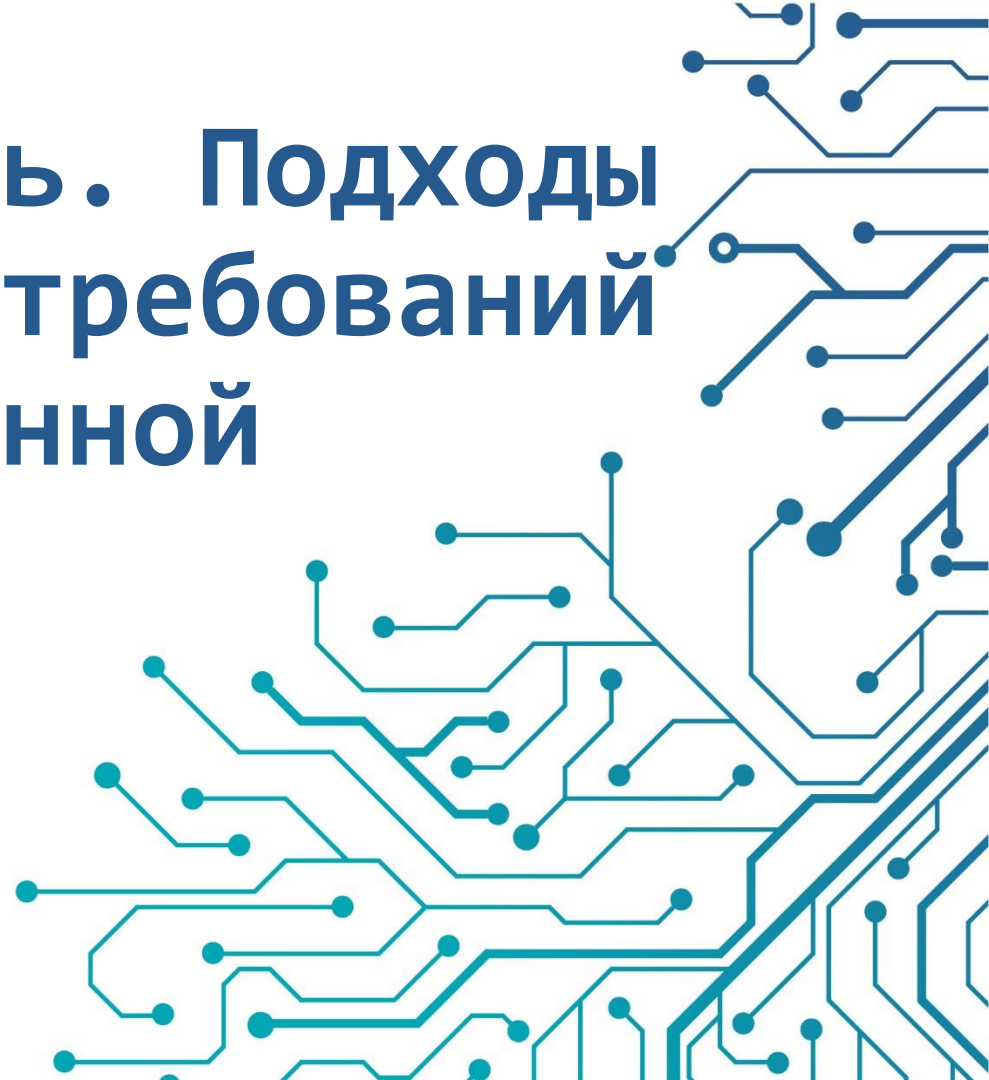
Цифровой рубль. Подходы к реализации требований по информационной безопасности

Бадмаева Римма
ведущий менеджер продуктов



infotecs

конференция РусКрипто

Назначение, возможности ЦР

Цифровой рубль – цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег

Формы национальной валюты:

- Наличная
- Безналичная
- Цифровая

Источник: официальный сайт Банка России

Нормативные документы по Цифровому Рублю

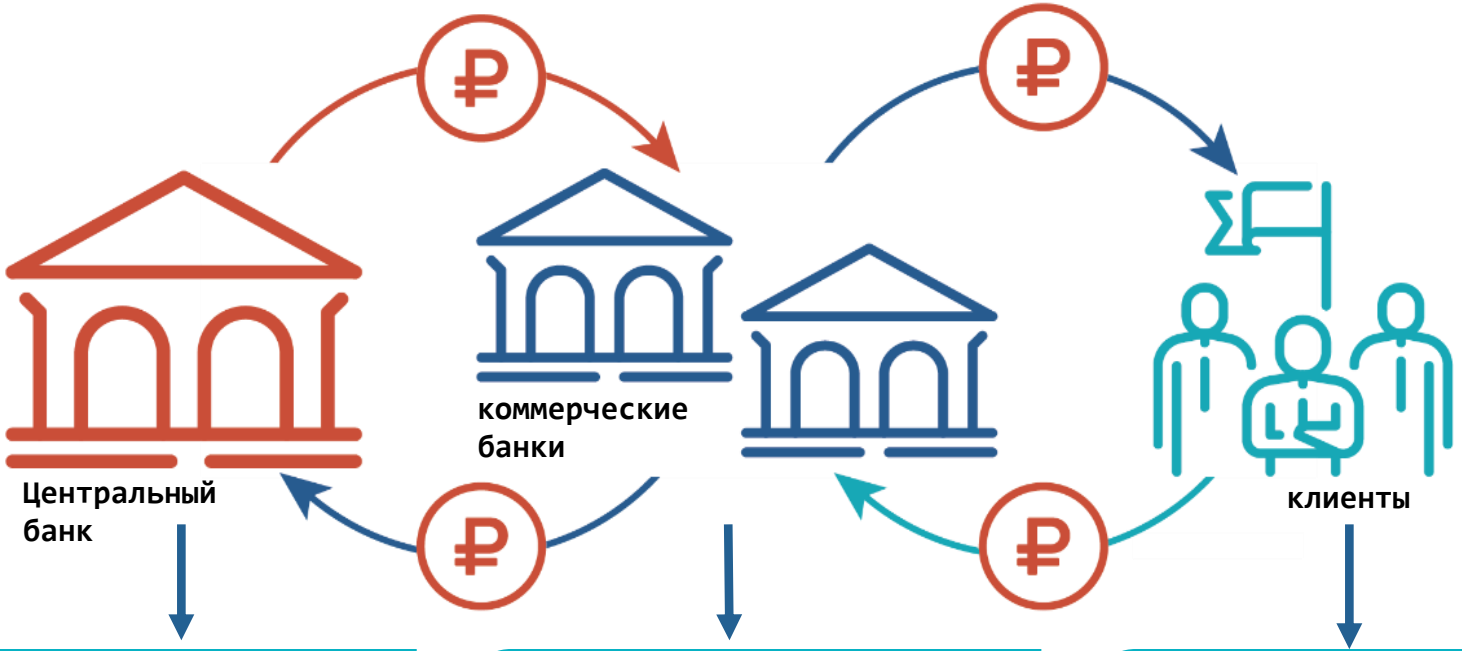
Положения Банка России:

- «О платформе цифрового рубля» **№820-П** от 03.08.2023
- «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» **№833-П** от 07.12.2023

Стандарты платформы цифрового рубля:

- ЦВЦБ. Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля. Версия 1.2
- Стандарт платформы цифрового рубля. «Порядок подключения участника платформы к платформе цифрового рубля» версия 1.3
- и другие, см. http://www.cbr.ru/fintech/dr/doc_dr/standarts/

Роли сторон в платформе ЦР

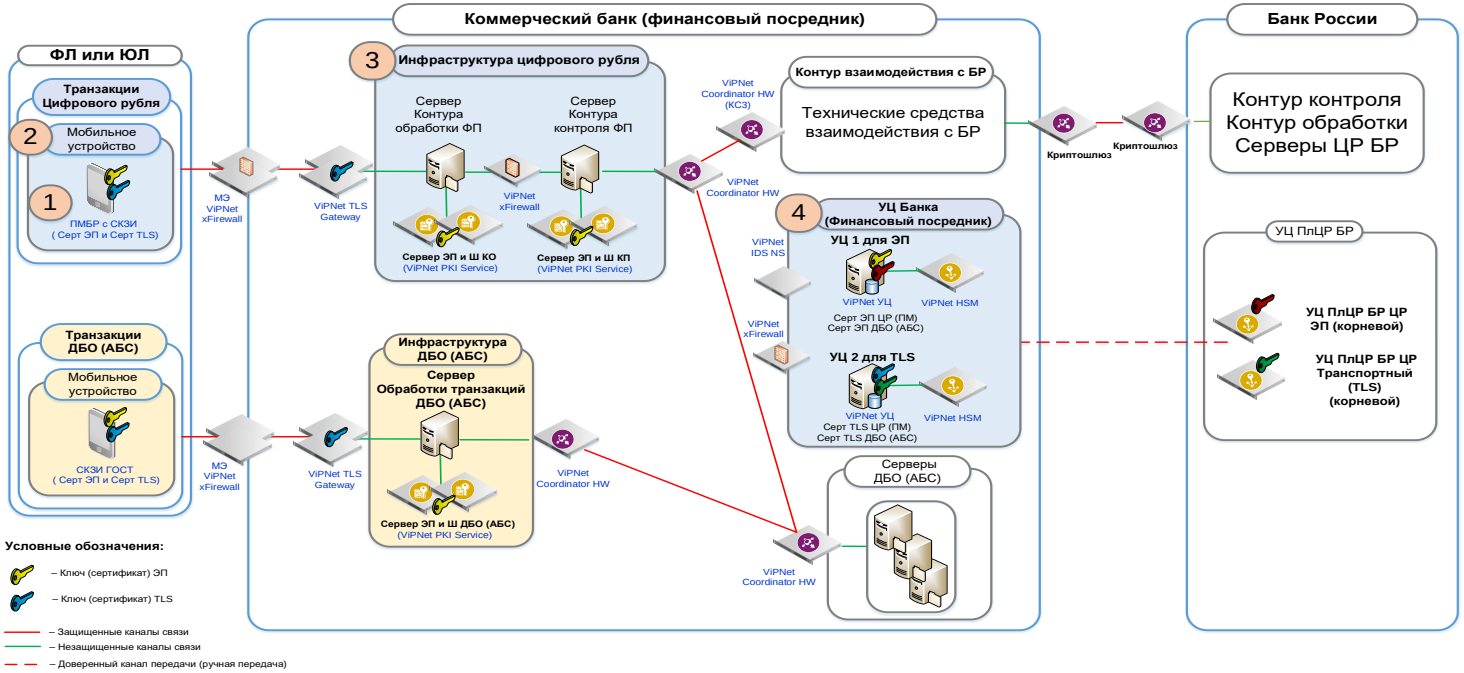


Оператор платформы

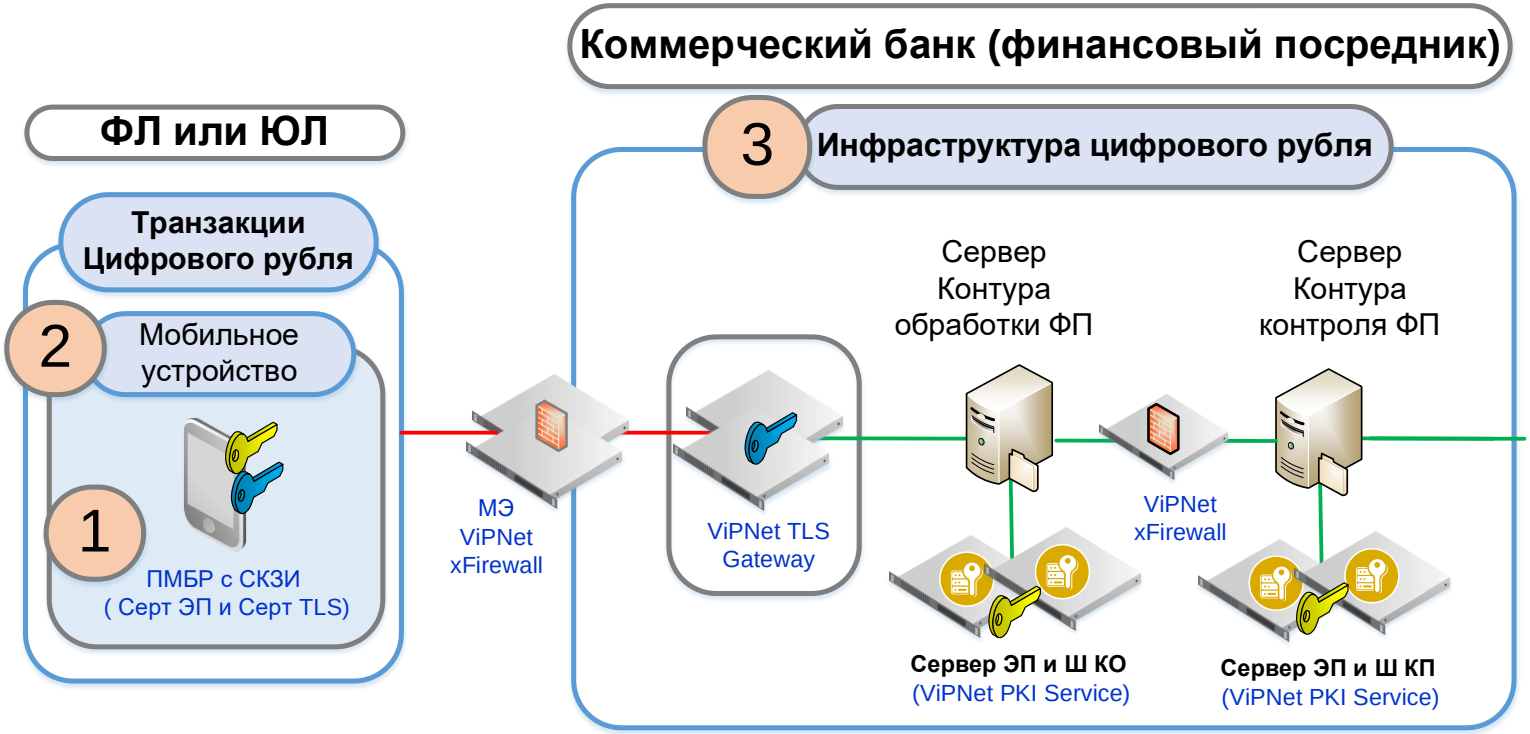
Участники платформы (Финансовые посредники)

Пользователи платформы (физ и юр лица)

СЗИ для защищенного взаимодействия участников платформы Цифрового рубля



1.Сегмент Пользователь – Банк



1.ПМ БР –

программный модуль Банка России

1.ПМ БР

Основа:

Ядро - СКЗИ ГОСТ (**ViPNet OSSL**, КриптоПро CSP, Валидата CSP)

«Надстройка» в виде API для работы СКЗИ с мобильным приложением банка

Функции:

- Создание запросов на сертификат
- Организация TLS-соединений
- Подпись сообщений
- Шифрование/расшифрование сообщений

1.ПМ БР: опыт ИнфоТеКС

ViPNet OSSL

ПМ БР (с ViPNet OSSL) – разработка АО «ИнфоТеКС» по заданию Банка России

ПМ БР - Исключительные права принадлежат Банку России

I Этап:

- Разработка ПМ БР с ViPNet OSSL 5.4 с фунциональностью ЭП и шифрования
- Передача банкам для встраивания в МП

II Этап:

- Разработка ПМ БР с ViPNet OSSL 5.4 с фунциональностью TLS
- Передача банкам для встраивания в МП

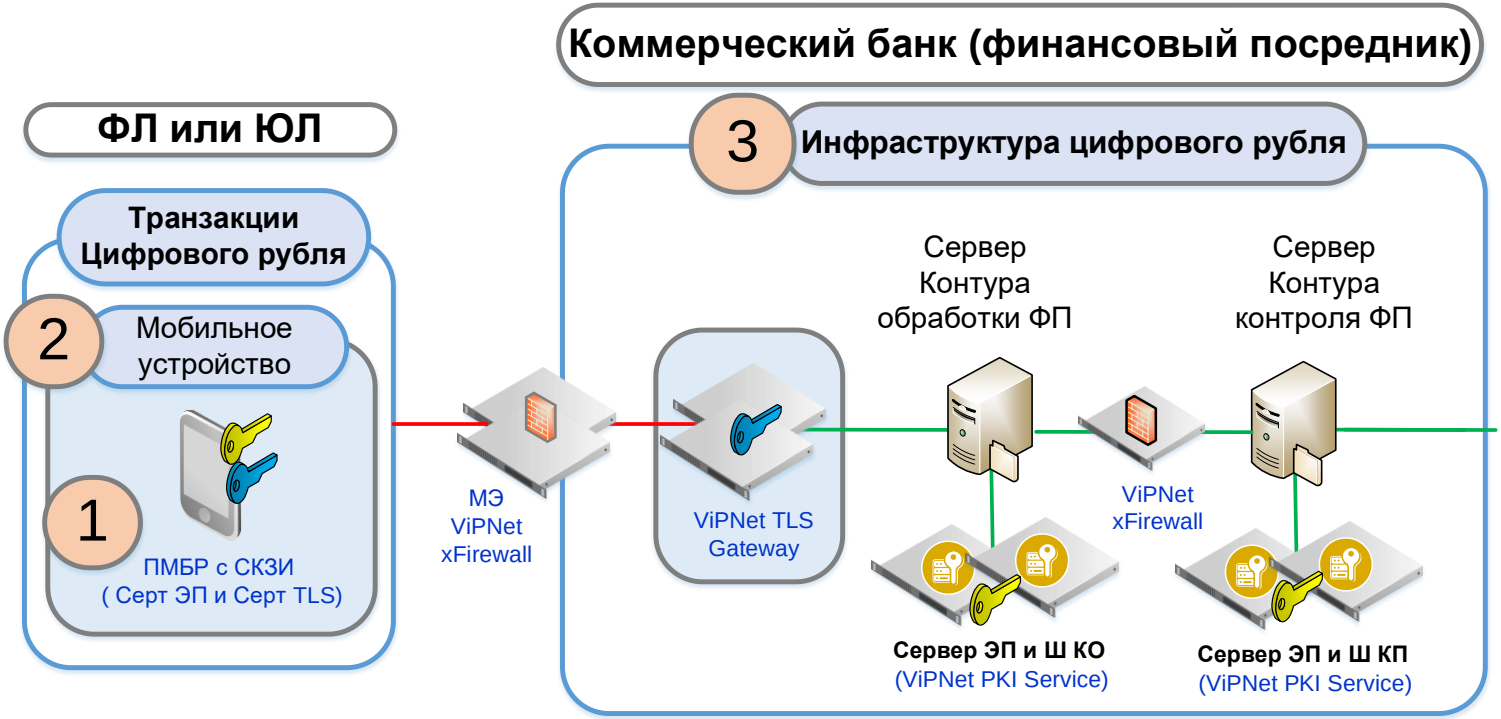
1. ViPNet OSSL – криптобиблиотека для встраивания

Сертифицированное СКЗИ и средство ЭП (КС1-КС3)

Особенности:

- Интерфейс OpenSSL для встраивания
- Содержит программный токен
- Поддержка актуальных форматов подписи, алгоритмов и протоколов
- Поддержка аппаратных токенов

2-3.Сегмент Пользователь – Банк



2-3.Сегмент Пользователь – Банк

На стороне банка:

- Организация TLS-соединений
- TLS шлюз класса КС2 (п.14.2, абз 6, 833-П, **вступают в силу с.1.01.2025**)

На устройстве пользователя:

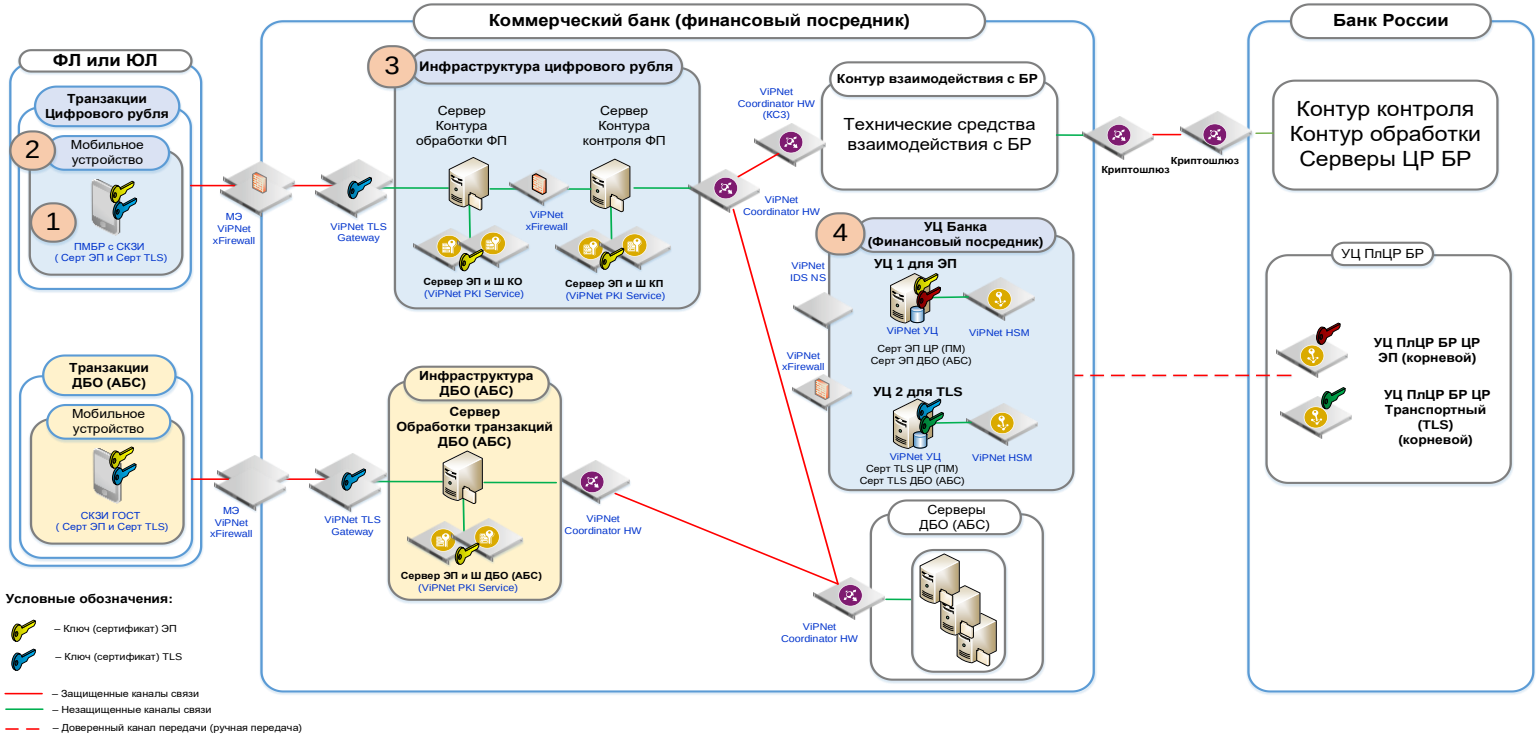
- Двусторонний TLS КС1 (п.14.2, абз.6, 833-П, **вступают в силу с.1.01.2025**)
- СКЗИ класса КС1 (п.14.2, абз.3, 833-П, **вступают в силу с.1.01.2025**)

2-3. ViPNet TLS Gateway – шлюз безопасности для ФП

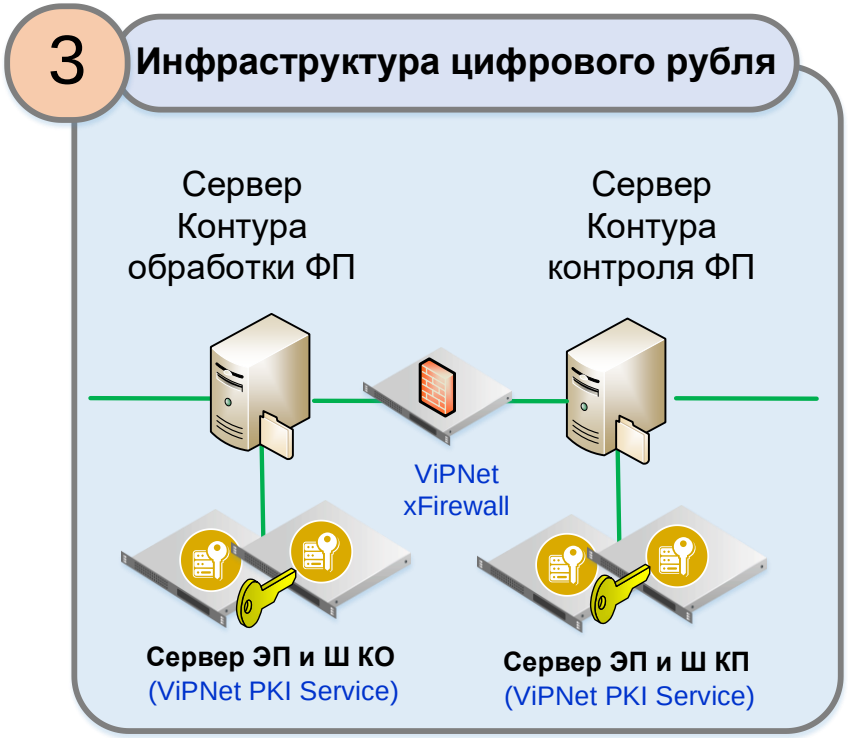
ViPNet TLS Gateway

- Легитимная **работа с любым СКЗИ** на стороне пользователя (ViPNet, КриптоПро, Валидата)
- Поддержка **дуального режима работы** (одновременная работа с использованием российских и иностранных криптоалгоритмов)
- **Высокая производительность** по кол-ву одновременных подключений (до **65 000 соединений**)
- **Полная линейка продуктов PKI**

3.Контур обработки. Контур контроля



3. Контур обработки. Контур контроля



СКЗИ:

- ViPNet PKI Service
- ViPNet PKI Client для АРМ Администратора

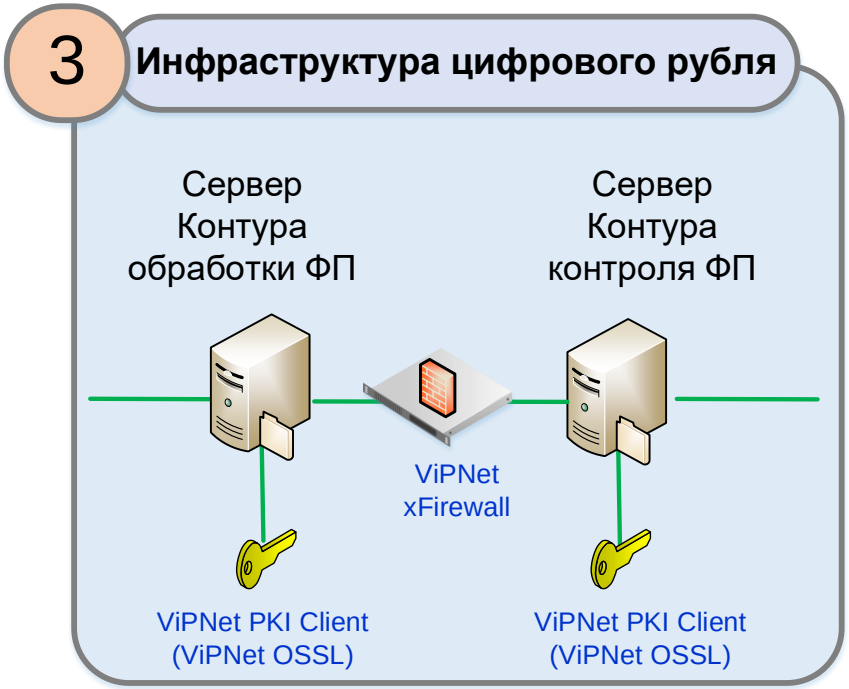
Решаемые в КО и КК задачи:

- Формирвоание/проверка ЭП
- Шифрование/расшифрование сообщений

Требования к серверу ЭП и Ш:

- УНЭП средствами ЭП не ниже КС3 (п.14.1, 833-П, **вступают в силу с 1.01.2025**)
- СКЗИ не ниже КС3 (п.14.1, 833П, **вступают в силу с 1.01.2025**)

3. Контур обработки. Контур контроля



Комплектация ЭкстраЭконом:

- PKI Client или OSSL вместо PKI Service

3.Контур обработки. Контур контроля

Важные Нюансы

Две ЭП: для контура обработки (КО)
и контура контроля (КК) **(п.4.1.2 порядка подключения)**

СКЗИ класса **КС3** для формирования/проверки ЭП
и шифрования/расшифрования сообщений

Используется **УНЭП** (не нужна аккредитация УЦ)

Требуется **оценка влияния**

3.ViPNet PKI Service – сервер подписи и шифрования для ФП

ViPNet PKI Service

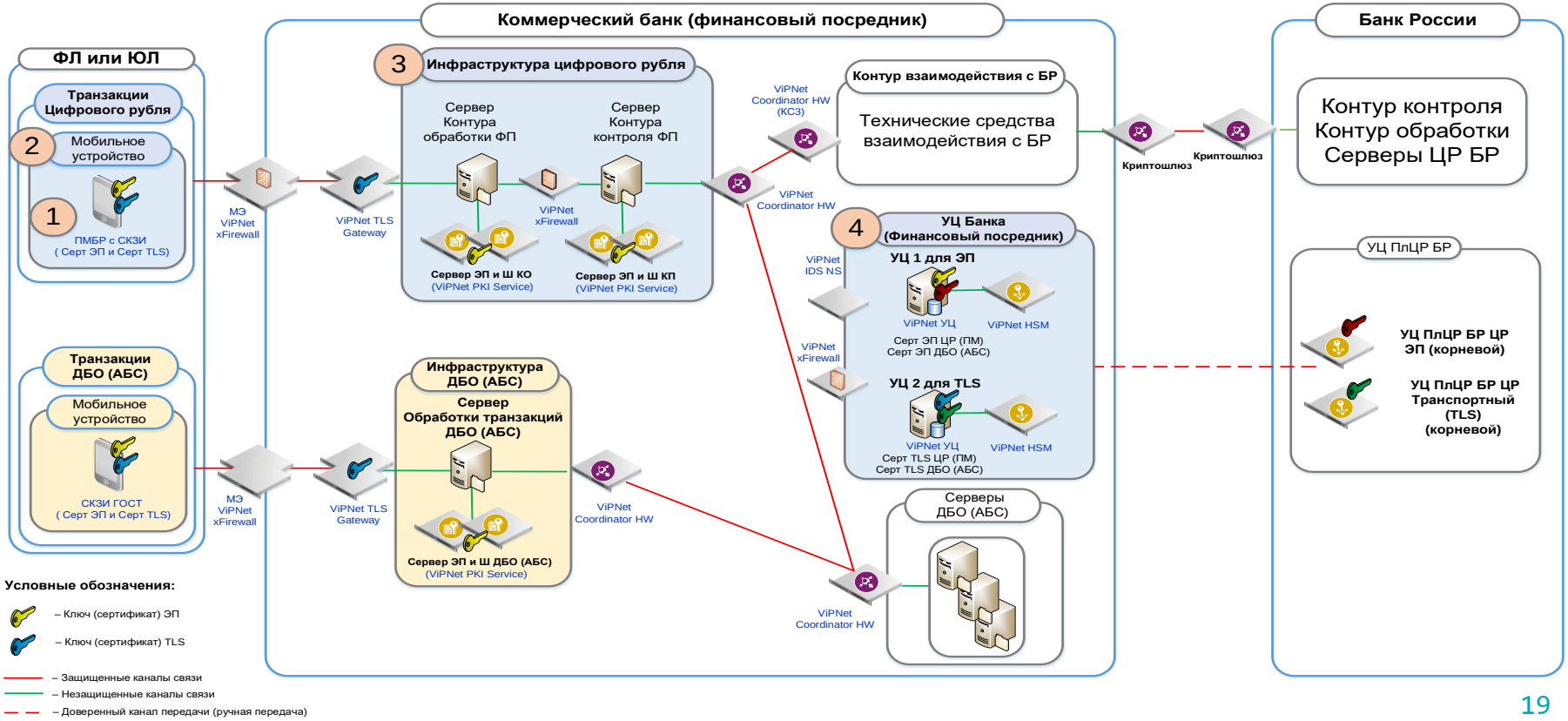
СКЗИ и средство ЭП **класса КВ/КВ2 со встроенным ФДСЧ и ДНСД**

Хранение ключей и сертификатов разных внешних систем в защищенном виде

Простота внедрения за счет наличия REST API для взаимодействия с сегментами КО и КК

Экономия за счет использования единой аппаратной платформы (сервис подписи и СКЗИ)

4.Удостоверяющие центры



4.Удостоверяющие центры

Средство УЦ:

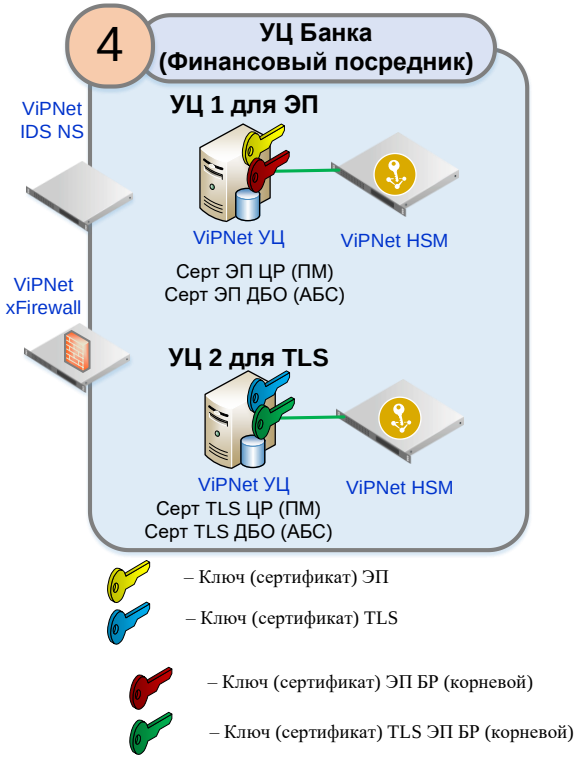
УЦ класса не ниже КС3 **(п. 13.4, П-833)**

Наличие HSM для хранения ключа ЭП

Решаемые задачи:

УЦ 1 - Выпуск сертификатов УНЭП

УЦ 2 – Выпуск сертификатов TLS



4. Удостоверяющие центры

Важные нюансы

- **Два отдельных УЦ** для сертификатов УНЭП и сертификатов TLS
- Ключ ЭП УЦ должен хранится **в HSM**
- **УЦ** – класса **КС3**
- **Аккредитация** УЦ **не требуется**

4. ViPNet УЦ – УЦ для ФП

ViPNet
Certification
Authority

Средство УЦ **класса КС3**

Поддержка **ViPNet HSM**

Низкая **стоимость владения УЦ,** стоимость лицензии на 1 ЭП – **10 рублей**

Работы встраиванию и оценки влияния ПМ БР в МП ФП, КО и КК

Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля

- Получить ПМ БР и выполнить **встраивание ПМ БР в Мобильное приложение ФП** в соответствии с порядком и требованиями на встраиваемый ПМ БР (П.3.4.2 Порядка подключения ФП)
- Проведение исследований по оценке влияния Мобильного приложения Финансового посредника на штатное функционирование ПМБР и СКЗИ

Требования по обеспечению информационной безопасности для Финансового посредника

- **Требования к АС ФП -** Для реализации бизнес-процессов ЦР во внутренних АС ФП требуется проведение **оценки влияния среды функционирования СКЗИ** в соответствии с требованиями документации на используемое СКЗИ и (7) (п.3.2.3 Мероприятий ИБ к Требованиям). Заключение по результатам оценке влияния среды функционирования СКЗИ

Требования к Мобильному приложению ФП

- **Оценка влияния среды функционирования ПМ БР** на выполнение предъявленных к СКЗИ требований в соответствии с документом (п.3.2.7 Мероприятий ИБ к Требованиям)

Работы встраивания и оценки влияния ПМ БР в МП ФП, КО и КК

Аккредитованная испытательная лабораторией в системах сертификации ФСБ России и ФСТЭК России, **имеющая право и опыт проведения тематических исследований** (сертификационных испытаний) программных и программно-аппаратных средств на соответствие требованиям ФСБ России к средствам криптографической защиты информации

Ответы на вопросы

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363

infotecs

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363